Dualization in Lattices Given by Ordered Sets of Irreducibles

Mikhail A. Babin, Sergei O. Kuznetsov

December 31, 2015

Abstract

Dualization of a monotone Boolean function on a finite lattice can be represented by transforming the set of its minimal 1 values to the set of its maximal 0 values. In this paper we consider finite lattices given by ordered sets of their meet and join irreducibles (i.e., as a concept lattice of a formal context). We show that in this case dualization is equivalent to the enumeration of so-called minimal hypotheses. In contrast to usual dualization setting, where a lattice is given by the ordered set of its elements, dualization in this case is shown to be impossible in output polynomial time unless P = NP. However, if the lattice is distributive, dualization is shown to be possible in subexponential time.

1 Introduction

A monotone Boolean function on a finite lattice can be given by the set of minimal 1 values or by the set of its maximal 0 values. Dualization is the transformation of the set of minimal 1 values of a Boolean function to the set of its maximal 0 values or vice versa. Since dualization is equivalent to many important problems in computer and data sciences [4, 19, 5], the paper [10] on quasi-polynomial dualization algorithm for Boolean lattices was an important breakthrough. It paved the way to generalizations to various classes of structures where dualization in output subexponential time is possible, among them dualization on lattices given by ordered sets of their elements or by products of bounded width lattices, like chains [4, 5].

A well-known fact is that every lattice is determined up to isomorphism by the ordered set of its meet (infimum) and join (supremum) irreducible elements [11]. These elements cannot be represented as meets (joins) of other elements that are larger (smaller) then them. On diagram of finite lattices these elements have one upper (lower) neighbor. In this paper we consider finite lattices given by ordered sets of their meet and join irreducibles, known as concept lattices [11, 1, 14]. We show that dualization for representation of this type is impossible in output polynomial time unless P = NP. However, in an important particular case where the lattice is distributive, we propose a subexponential algorithm.

Dualization in the considered case is not only of theoretical interest. Actually, this study was motivated by a practical problem of enumerating minimal hypotheses, which is a problem

of learning specific type of classifiers from positive and negative examples. Hypotheses or JSM-hypotheses were proposed by V.K.Finn [8, 9] and formalized in terms of Formal Concept Analysis (FCA) in [16, 13, 17]. The set of minimal hypotheses is classification equivalent to the set of all hypotheses, thus making a condensed representation of the latter. The set of all hypotheses can be generated with polynomial delay [17], however, the problem of generating minimal hypotheses with polynomial delay remained an open one for long time. In this paper we show that dualization on lattices given by the ordered set of its irreducible elements is equivalent to enumeration of minimal hypotheses, thus complexity results concerning minimal hypotheses and dualization can be mutually translated.

In what follows we shall use the notation of Formal Concept Analysis [11], which provides a convenient language and necessary results for lattices given by ordered sets of irreducible elements.

The rest of the paper is organized as follows: In the second section we give most important definitions. In the third section we prove the main intractability result on impossibility of enumerating minimal hypotheses and dualization in output polynomial time unless P = NP. In the fourth section we conclude by discussing the implication of the results for the problem of dualizing monotone Boolean functions. In the fifth section we relate minimum implication base problem to dualization over product of lattices that are given explicitly, and dualization over distributive lattice. In the sixth section we describe subexponential dualization algorithm for the distributive lattice case.

1.1 Related work

To the best of our knowledge all dualization problems that have been studied in previous works consider dualization over product of posets $\mathcal{P} = \mathcal{P}_1 \times \ldots \times \mathcal{P}_k$, where each poset $\mathcal{P}_i$ is some special type of a poset that is given explicitly. In [5, 7] the author give quasi-polynomial time algorithms for the following cases: each $\mathcal{P}_i$ is a join semi-lattice of bounded width (any antichain has constant size), each $\mathcal{P}_i$ is a forest poset in which either the in-degree or the out-degree of each element is constant (see also [6]), each $\mathcal{P}_i$ is the lattice of intervals defined by a set of intervals on the real line $\mathbb{R}$. In [5, 7] a more general dualization problem was stated where each $\mathcal{P}_i$ is a lattice (with no bounds on its width), the existence of quasi-polynomial time algorithms for this case is still an open question. In this paper we prove an upper bound complexity of the latter problem via another long-standing open complexity problem, the minimum implication base (see [2], equivalently SID problem from [21, 4]). The most common technique leading to quasi-polynomial time algorithm for duality problems are based on the idea of high frequency based decomposition, first introduced in [10]. We use this method to get subexponential algorithm for the dualization over distributive lattice.

Although product of lattices $\mathcal{L} = \mathcal{L}_1 \times \ldots \times \mathcal{L}_k$, where each $\mathcal{L}_i$ is given explicitly, can provide exponentially smaller description of $\mathcal{L}$ not every lattice can have a nontrivial exponentially smaller representation of this kind.

2 Preliminaries

Definition 2.1. [1] *A subset $\mathcal{A} \subseteq \mathcal{P}$ of a partially ordered set $(\mathcal{P}, <)$ is called an* antichain *iff $A \not\leq B$ for any $A, B \in \mathcal{A}$, i.e., all elements of an antichain are incomparable.*

The following property is required in dualization problems. For two antichains $\mathcal{A}, \mathcal{B} \subseteq \mathcal{P}$ we say $(\mathcal{A}, \mathcal{B})$ has property $(*)$ if

$$A \not\leq B \text{ for any } A \in \mathcal{A},\ B \in \mathcal{B}\ (*).$$

Definition 2.2. *Antichains $\mathcal{A}, \mathcal{B} \subseteq \mathcal{P}$ of partially ordered set $\mathcal{P}$ are called dual iff $\mathcal{A}, \mathcal{B}$ satisfy property (*) and for any $P \in \mathcal{P}$ either $P \leq B$ for some $B \in \mathcal{B}$ or $A \leq P$ for some $A \in \mathcal{A}$.*

The dualization problem over partially ordered set usually have the following statement:
Problem: Dualization over partially ordered set $\mathcal{P}$
INPUT: Partially ordered set $\mathcal{P}$ (that can be given implicitly), antichain $\mathcal{A} \subseteq \mathcal{P}$.
OUTPUT: Antichain $\mathcal{B} \subseteq \mathcal{P}$ such that $\mathcal{A}$ and $\mathcal{B}$ are dual.

Note that the output $\mathcal{B}$ of the dualization problem can be exponential in the input size ($|\mathcal{A}| \times |[description\ of\ \mathcal{P}]|$). Therefore, we are interested in the time complexity of dualization that depends on both input and output sizes. We say that dualization problem can be solved in *output polynomial* time if there is an algorithm that can generate set $\mathcal{B}$ in time polynomial of $|\mathcal{B}| \times |\mathcal{A}| \times |[description\ of\ \mathcal{P}]|$. Usually we will consider decision version of the dualization problem called *duality* problem:
Problem: Duality over partially ordered set $\mathcal{P}$
INPUT: Partially ordered set $\mathcal{P}$ (that can be given implicitly), antichains $\mathcal{A}, \mathcal{B} \subseteq \mathcal{P}$ satisfying (*).
QUESTION: Are antichains $\mathcal{A}$ and $\mathcal{B}$ dual?

Equivalent definition of the dualization over poset can be given using monotone Boolean[2] functions on a partially ordered set. Let $f : \mathcal{P} \mapsto \{0, 1\}$ be a monotone Boolean function on a partially ordered set $\mathcal{P}$, i.e. $X \leq Y \Rightarrow f(X) \leq f(Y)$ and $\mathcal{A}$ is a set of minimal 1-values of f. Clearly, the set of maximal 0-values of f is dual to $\mathcal{A}$.

In this paper we consider only the case where the partially ordered set over which we dualize is a lattice. A partial ordered set $(\mathcal{L}, <)$ is called a *lattice* [1] if any pair of its elements has an infimum (meet $\wedge$) and a supremum (join $\vee$). Equivalently, a lattice is an algebra $(\mathcal{L}, \wedge, \vee)$ with the following properties of $\wedge$ and $\vee$:

L1 $X \vee X = X, \quad X \wedge X = X$ (idempotence)

L2 $X \vee Y = Y \vee X, \quad X \wedge Y = Y \wedge X$ (commutativity)

L3 $X \vee (Y \vee Z) = (X \vee Y) \vee Z, \quad X \wedge (Y \wedge Z) = (X \wedge Y) \wedge Z$ (associativity)

L4 $X = X \wedge (X \vee Y) = X \vee (X \wedge Y)$ (absorption)

[1] We use capital characters to denote elements of partially ordered sets since it agrees with FCA notation for concept lattices.

[2] Hereafter by Boolean functions we mean Boolean-valued functions.

A lattice is called *complete* if every subset of it has infimum and supremum.

A lattice is distributive if for any $X, Y, Z \in \mathcal{L}$

$$X \wedge (Y \vee Z) = (X \wedge Y) \vee (X \wedge Z).$$

The following elements of a lattice are very important in our work. An element $X \in \mathcal{L}$ is called *infimum-irreducible* (or *meet-irreducible*) if $X \neq \bigwedge_{Y>X} Y$, i.e., X is not represented by the intersection of any elements above it. Dually, an element $X \in \mathcal{L}$ is called *supremum-irreducible* (or *join-irreducible*) if $X \neq \bigvee_{Y<X} Y$, i.e., X is not represented by the union of any elements below it. Meet- (join-) irreducible elements have only one upper (lower) neighbor in the lattice diagram.

In what follows we use the standard definitions and facts of Formal Concept Analysis (FCA) from [11]. Let G and M be sets, called the set of *objects* and *attributes*, respectively. Let I be a relation $I \subseteq G \times M$ between objects and attributes: for $g \in G, m \in M, gIm$ holds iff the object g has the attribute m. The triple $\mathbb{K} = (G, M, I)$ is called a *(formal) context* and is naturally represented by a cross-table, where rows stay for objects, columns stay for attributes and crosses stay for pairs $(g, m) \in I$. If $A \subseteq G, B \subseteq M$ are arbitrary subsets, then the following *derivation operators*

$$A' = \{m \in M \mid gIm \ \forall g \in A\}$$

$$B' = \{g \in G \mid gIm \ \forall m \in B\}$$

define *Galois connection* between ordered powersets $(2^G, \subseteq)$ and $(2^M, \subseteq)$, since $A \subseteq B' \iff B \subseteq A'$. The pair (A, B), where $A \subseteq G$, $B \subseteq M$, $A' = B$, and $B' = A$ is called a *(formal) concept (of the context $\mathbb{K}$)* with *extent* A and *intent* B (in this case we have also $A'' = A$ and $B'' = B$). Formal concepts are ordered by the following relation

$$(A_1, B_1) \leq (A_2, B_2) \text{ iff } A_1 \subseteq A_2 (B_2 \subseteq B_1),$$

this partial order being a complete lattice on the set of all concepts. This lattice is called a *concept lattice* $\mathcal{L}(G, M, I)$ of the context (G, M, I).

The set of join-irreducible elements of a concept lattice $\mathcal{L}(G, M, I)$ is contained in the set of *object concepts*, which have the form (g'', g'), $g \in G$. Dually, the set of meet-irreducible elements of a concept lattice is contained in the set of *attribute concepts*, which have the form (m', m''), $m \in M$. An object g is called *reducible* if $g' = M$ or $\exists X \subseteq G \setminus \{g\} : \ g' = \bigcap_{j \in X} j'$, i.e., the respective row of the context cross-table is either full or is an intersection of some other rows. If g is not reducible, then (g'', g') is a join-irreducible element of $\mathcal{L}(G, M, I)$. Dually, an attribute m is called *reducible* if $m' = G$ or $\exists Y \subseteq M \setminus \{m\} : \ m' = \bigcap_{j \in Y} j'$, i.e. the respective column of the context cross-table is either full or is an intersection of some other columns. If m is not reducible, then (m', m'') is a meet-irreducible element of $\mathcal{L}(G, M, I)$.

The Basic Theorem of FCA [11] implies that every finite lattice $(L, \vee, \wedge)$ can be represented as a concept lattice $\mathcal{L}(J(L), M(L), \leq)$, where $J(L)$ is the set of all join-irreducible elements of L, $M(L)$ is the set of meet-irreducible elements of L, and $\leq$ is the natural partial order of $(L, \vee, \wedge)$.

A set of attributes B is *implied* by a set of attributes A, or implication $A \to B$ holds, if all objects from G that have all attributes from A also have all attributes from B, i.e. $A' \subseteq B'$. Implications obey Armstrong rules

$$\frac{}{X \to X} \quad , \quad \frac{X \to Y}{X \cup Z \to Y} \quad , \quad \frac{X \to Y, Y \cup Z \to W}{X \cup Z \to W},$$

and a minimal subset of implications from which all other implications can be deduced by means of Armstrong rules is called an *implication base*. In [2] a characterization of cardinality-minimum implication base (Duquenne-Guigues base) was given.

3 Enumeration of minimal hypotheses

Now we present a learning model from [8, 9] in terms of FCA [16, 13, 17]. This model complies with the common paradigm of learning from positive and negative examples (see, e.g. [13], [17]): given a positive and negative examples of a "target attribute", construct a generalization of the positive examples that would not cover any negative example.

Let t be *target* attribute, different from attributes from the set M, which correspond to *structural* attributes of objects. For example, in pharmacological applications the structural attributes can correspond to particular subgraphs of molecular graphs of chemical compounds.

Input data for learning can be represented by sets of positive, negative, and undetermined examples. *Positive examples* (or $(+)$-examples) are objects that are known to have the target attribute t and *negative examples* (or $(-)$-examples) are objects that are known not to have this attribute.

Definition 3.1. *Consider positive context* $\mathbb{K}_+ = (G_+, M, \mathcal{I}_+)$ *and negative context* $\mathbb{K}_- = (G_-, M, \mathcal{I}_-)$. *The context* $\mathbb{K}_\pm = (G_+ \cup G_-, M \cup \{w\}, \mathcal{I}_+ \cup \mathcal{I}_- \cup G_+ \times \{w\})$ *is called a* training context. *The derivation operators in these contexts are denoted by superscripts* $(\cdot)^+$, $(\cdot)^-$, *and* $(\cdot)^\pm$, *respectively.*

Definition 3.2. *A subset* $H \subseteq M$ *is called a positive (or* $(+)$*-)-hypothesis of training context* $\mathbb{K}_\pm$ *if* H *is intent of* $\mathbb{K}_+$ *and* H *is not a subset of any intent of* $\mathbb{K}_-$. *For* $k \in N \cup \{0\}$ *a subset* $H \subseteq M$ *is called a* k*-weak positive (or* $k(+)$*-)-hypothesis of training context* $\mathbb{K}_\pm$ *if* H *is intent of* $\mathbb{K}_+$ *and* $|H^+ \cap G_-| \leq k$.

Obviously, a positive hypothesis is a 0-weak hypothesis. Weak hypotheses stay for noise-tolerant dependencies, which are important in data mining applications. In the same way negative (or $(-)$-) hypotheses are defined.

Besides classified objects (positive and negative examples), one usually has objects for which the value of the target attribute is unknown. These examples are usually called undetermined examples, they can be given by a context $\mathbb{K}_\tau := (G_\tau, M, I_\tau)$, where the corresponding derivation operator is denoted by $(\cdot)^\tau$.

Hypotheses can be used to classify the undetermined examples: If the intent

$$g^\tau := \{m \in M \mid (g, m) \in I_\tau\}$$

of an object $g \in G_\tau$ contains a positive, but no negative hypothesis, then g^τ is *classified positively*. Negative classifications are defined similarly. If g^τ contains hypotheses of both kinds, or if g^τ contains no hypothesis at all, then the classification is contradictory or undetermined, respectively. In this case one can apply probabilistic techniques.

In [13], [17] it was argued that one can restrict to *minimal* (w.r.t. inclusion $\subseteq$) hypotheses, positive as well as negative, since an object intent g^τ obviously contains a positive hypothesis if and only if it contains a minimal positive hypothesis.

Definition 3.3. *For $k \in \mathbb{N} \cup \{0\}$ if the set of $k(+)$-hypotheses is not empty, then H is a minimal $k(+)$-hypothesis iff H is a $k(+)$-hypothesis and F is not a $k(+)$-hypothesis for any $F \subset H$. In case the set of $k(+)$-hypotheses is empty, we put the set of minimal $k(+)$-hypotheses consisting of the only set M.*

The latter condition is needed technically for dualization: without it not every monotone Boolean function would be dualizable.

Example. Consider the following training context, where m_0 is the target attribute, the set of attributes is $M = \{m_1, \ldots, m_6\}$, the set of negative examples is $G = \{g_1, g_2, g_3\}$, the set of positive examples is $G_+ = \{g_4, \ldots, g_9\}$ and the incidence relation I is given by the following cross-table:

$G \setminus M$	m_0	m_1	m_2	m_3	m_4	m_5	m_6
g_1			×	×		×	×
g_2		×		×	×		×
g_3		×	×		×	×	
g_4	×		×	×	×	×	×
g_5	×	×		×	×	×	×
g_6	×	×	×		×	×	×
g_7	×	×	×	×		×	×
g_8	×	×	×	×	×		×
g_9	×	×	×	×	×	×	

Here, we have $2^3 = 8$ minimal hypotheses: $\{m_1, m_2, m_3\}$, $\{m_1, m_2, m_6\}$, $\{m_1, m_5, m_3\}$, $\{m_1, m_5, m_6\}$, $\{m_4, m_2, m_3\}$, $\{m_4, m_2, m_6\}$, $\{m_4, m_5, m_3\}$, $\{m_4, m_5, m_6\}$.

In what follows we will also need the following definition from FCA, which is important in constructing "hard cases" for FCA-related complexity problems.

Definition 3.4. *Let $G = \{g_1, \ldots, g_n\}$ and $M = \{m_1, \ldots, m_n\}$ be sets with same cardinality. Then the context $\mathbb{K} = (G, M, \mathcal{I}_{\neq})$ is called* contranominal scale*, where $\mathcal{I}_{\neq} = G \times M \setminus \{(g_1, m_1), \ldots, (g_n, m_n)\}$.*

The contranominal scale has the following property, which we will use later: for any $H \subseteq M$ one has $H'' = H$ and $H' = \{g_i \mid m_i \notin H, 1 \leq i \leq n\}$.

Here we discuss algorithmic complexity of enumerating all minimal hypotheses. Note that there is an obvious algorithm for enumerating all hypotheses (not necessary minimal) with polynomial delay [17]. This algorithm is an adaptation of an algorithm for computing

the set of all concepts, where the branching condition is changed to include the additional condition $|H^+ \cap G_-| \leq k$.

Problem: Minimal hypotheses enumeration (MHE)
INPUT: Positive and negative contexts $\mathbb{K}_+ = (G_+, M, \mathcal{I}_+), \mathbb{K}_- = (G_-, M, \mathcal{I}_-)$
OUTPUT: All minimal hypotheses of $\mathbb{K}_\pm$.

Unfortunately, this problem cannot be solved in output polynomial time unless $P = NP$. In order to prove this result we study complexity of the following decision problem.

Problem: Additional minimal hypothesis (AMH)
INPUT: Positive and negative contexts $\mathbb{K}_+ = (G_+, M, \mathcal{I}_+), \mathbb{K}_- = (G_-, M, \mathcal{I}_-)$ and a set of minimal hypotheses $\mathcal{H} = \{H_1, \ldots, H_k\}$.
QUESTION: Is there an *additional* minimal hypothesis H of $\mathbb{K}_\pm$ i.e. minimal hypothesis H such that $H \notin \mathcal{H}$.

Algorithm 1 FindNewMinH($\mathbb{K}_+, \mathbb{K}_-, \mathcal{H}$)

Require: DecideAMH($\mathbb{K}_+, \mathbb{K}_-, \mathcal{H}$) = **true**
1: **for** $g \in G_+$ **do**
2: $G^g_+ \Leftarrow \{g^+ \cap h^+ \mid h \in G_+\}$
3: $I^g_+ \Leftarrow \{(g, m) \mid m \in g, g \in G^g_+\}$
4: $G^g_- \Leftarrow \{g^+ \cap h^- \mid h \in G_-\}$
5: $I^g_- \Leftarrow \{(g, m) \mid m \in g, g \in G^g_-\}$
6: $\mathbb{K}^g_+ \Leftarrow \mathbb{K}(G^g_+, M \cap g^+, I^g_+)$
7: $\mathbb{K}^g_- \Leftarrow \mathbb{K}(G^g_-, M \cap g^+, I^g_-)$
8: $\mathcal{H}^g \Leftarrow \{h \mid h \subseteq g^+, h \in \mathcal{H}\}$
9: **if** DecideAMH($\mathbb{K}^g_+, \mathbb{K}^g_-, \mathcal{H}^g$) **then**
10: **return** FindNewMinH($\mathbb{K}^g_+, \mathbb{K}^g_-, \mathcal{H}^g$)
11: **end if**
12: **end for**
13: **return** M

Lemma 3.1. *AMH is in P iff MHE can be solved in output polynomial time.*

Proof. ($\Leftarrow$) Assume there is an output polynomial algorithm $\mathcal{A}$ that generates all minimal hypotheses in time $p(|G_+|, |M|, |\mathcal{I}_+|, |G_-|, |\mathcal{I}_-|, N)$, where N is the number of minimal hypotheses. Use this algorithm to construct $\mathcal{A}'$ that makes first $p(|G_+|, |M|, |\mathcal{I}_+|, |G_-|, |\mathcal{I}_-|, k+1)$ steps of $\mathcal{A}$. Clearly, if there is more than k minimal hypotheses, then $\mathcal{A}'$ generates $k+1$ minimal hypotheses, hence we can solve AMH in polynomial time.

($\Rightarrow$) Now suppose there is a function DecideAMH $(\mathbb{K}_+, \mathbb{K}_-, \mathcal{H})$ that solves AMH problem instance in time $O(t)$. We can use *Algorithm 1* to find an additional minimal hypothesis if there is one. Clearly `line` 2 to `line` 8 can be computed in time $O((|G_+| + |G_-|)|M|)$. Also note that the total number of recursive calls can not be greater than $|M|$. Thus, time complexity of the *Algorithm 1* is $O((|G_+| + |G_-|)|M|^2 t)$. Let us prove the correctness. First note that since hypotheses are closed in $\mathbb{K}_+$ the additional minimal hypothesis must be a subset of some $g^+, g \in G_+$, or it could be M. By definition the context $\mathbb{K}^g_+$ defines exactly all closed sets of $\mathbb{K}$ that are subsets of g^+. It remains to note that at the last recursive call of

Algorithm 1 DecideAMH($\mathbb{K}^g_+, \mathbb{K}^g_-, \mathcal{H}^g$) does not hold for any $g \in G_+$. Thus, the only possible additional minimal hypothesis that can be returned is M. □

Now we prove NP-completeness of AMH through the reduction of the most known NP-complete problem – satisfiability of CNF – to AMH.

Problem: CNF satisfiability (SAT)
INPUT: A Boolean CNF formula $f(x_1, \ldots, x_n) = C_1 \wedge \ldots \wedge C_k$
QUESTION: Is f satisfiable?

Consider an arbitrary CNF instance $C_1, \ldots, C_k$ with variables $x_1, \ldots, x_n$, where $C_i = (l_{i_1} \vee \ldots \vee l_{ir_i}), 1 \leq i \leq k$ and $l_{ij} \in \{x_1, \ldots, x_n\} \cup \{\neg x_1, \ldots, \neg x_n\}$ $(1 \leq i \leq k,\ 1 \leq j \leq r_i)$ are literals, i.e., variables or their negations. From this instance we construct a positive context $\mathbb{K}_+ = (G_+, M, \mathcal{I}_+)$ and a negative context $\mathbb{K}_- = (G_-, M, \mathcal{I}_-)$. Define

$$M = \{C_1, \ldots, C_k\} \cup \{x_1, \neg x_1, \ldots, x_n, \neg x_n\}$$

$$G_+ = \{g_{x_1}, g_{\neg x_1}, \ldots, g_{x_n}, g_{\neg x_n}\} \cup \{g_{C_1}, \ldots, g_{C_k}\}$$

$$G_- = \{g_{l_1}, \ldots, g_{l_n}\}$$

The incidence relation of the positive context is defined by $\mathcal{I}_+ = \mathcal{I}_{\mathcal{C}} \cup \mathcal{I}_{\neq} \cup \mathcal{I}_{=}$, where

$$\begin{aligned}\mathcal{I}_{\mathcal{C}} = &\{(g_{x_i}, C_j) \mid x_i \notin C_j, 1 \leq i \leq n, 1 \leq j \leq k\} \\ &\cup \{(g_{\neg x_i}, C_j) \mid \neg x_i \notin C_j, 1 \leq i \leq n, 1 \leq j \leq k\}\end{aligned}$$

$$\begin{aligned}\mathcal{I}_{\neq} = &\{g_{x_1}, g_{\neg x_1}, \ldots, g_{x_n}, g_{\neg x_n}\} \times \{x_1, \neg x_1, \ldots, x_n, \neg x_n\} \\ &- \{(g_{x_1}, x_1), (g_{\neg x_1}, \neg x_1), \ldots, (g_{x_n}, x_n), (g_{\neg x_n}, \neg x_n)\}\end{aligned}$$

$$\mathcal{I}_{=} = \{(g_{C_1}, C_1), \ldots, (g_{C_k}, C_k)\}$$

that is for i-th clause $C_i^+ \cap \{g_{x_1}, g_{\neg x_1}, \ldots, g_{x_n}, g_{\neg x_n}\}$ is the set of literals not included in C_i, $\mathcal{I}_{\neq}$ is the relation of contranominal scale.

The incidence relation of the negative context is given by $\mathcal{I}_- = \mathcal{I}_{\mathcal{L}}$ where

$$\begin{aligned}\mathcal{I}_{\mathcal{L}} = &G_- \times \{x_1, \neg x_1, \ldots, x_n, \neg x_n\} \\ &- \{(g_{l_1}, x_1), (g_{l_1}, \neg x_1), \ldots, (g_{l_n}, x_n), (g_{l_n}, \neg x_n)\}\end{aligned}$$

.

		$C_1\ C_2\ \cdots\ C_k$	$x_1\ \neg x_1\ \cdots\ x_n\ \neg x_n$
$\mathbb{K}_+$	g_{x_1} $g_{\neg x_1}$ $\vdots$ g_{x_n} $g_{\neg x_n}$	$\mathcal{I}_{\mathcal{C}}$	$\mathcal{I}_{\neq}$
	g_{C_1} $\vdots$ g_{C_k}	$\mathcal{I}_{=}$	
$\mathbb{K}_-$	g_{l_1} $\vdots$ g_{l_n}		$\mathcal{I}_{\mathcal{L}}$

As the set of minimal hypotheses we take $\mathcal{H} = \{\{C_1\}, \{C_2\}, \ldots, \{C_k\}\}$. It is easy to see that $\mathbb{K}_\pm$ with $\mathcal{H}$ is a correct instance of AMH.

If a hypothesis (not necessary minimal) is not contained in $\mathcal{H}$ we will call it *additional*.

Proposition 3.2. *If H is an additional minimal hypothesis of $\mathbb{K}_\pm$ then $H \subseteq \{x_1, \neg x_1, \ldots, x_n, \neg x_n\}$.*

Proof. Suppose $H \nsubseteq \{x_1, \neg x_1, \ldots, x_n, \neg x_n\}$, then since H is not empty there is some $C_i \in H$, $1 \leq i \leq k$. But H is a minimal hypothesis and thus it does not contain any hypothesis. Hence $H = C_i$ and this contradicts the fact that H is an *additional* minimal hypothesis. □

For any $H \subseteq \{x_1, \neg x_1, \ldots, x_n, \neg x_n\}$ that satisfies $\{x_i, \neg x_i\} \cap H \neq \emptyset$ for any $1 \leq i \leq n$ we define the truth assignment φ_H in a natural way:

$$\varphi_H(x_i) = \begin{cases} true, & \text{if } x_i \in H; \\ false, & \text{if } x_i \notin H; \end{cases}$$

In the case $\{x_i, \neg x_i\} \cap H = \emptyset$ for some $1 \leq i \leq n$, φ_H is not defined. We define $\varphi_H(x_i) = true$ even if $\{x_i, \neg x_i\} \subseteq H$, although in this case it can be defined by eigther way.

Symmetrically, for a truth assignment φ define the set $H_\varphi = \{x_i \mid \varphi(x_i) = true\} \cup \{\neg x_i \mid \varphi(x_i) = false\}$.

Below, for $H \subseteq \{x_1, \neg x_1, \ldots, x_n, \neg x_n\}$ we will denote the complement of H in $\{x_1, \neg x_1, \ldots, x_n, \neg x_n\}$ by $\overline{H}$.

Proposition 3.3. *If a subset $H \subseteq \{x_1, \neg x_1, \ldots, x_n, \neg x_n\}$ is not contained in the intent of any negative example (i.e $\forall g \in G_-, H \nsubseteq g^-$), then $\varphi_{\overline{H}}$ is defined. Conversely, for a truth assignment φ the set $\overline{H_\varphi}$ is not contained in the intent of any negative concept.*

The proof is straightforward.

The following theorem proves NP-hardness of AMH.

Theorem 3.4. *AMH has a solution if and only if SAT has a solution.*

Proof. ($\Rightarrow$) Let H be an additional minimal hypothesis of $\mathbb{K}_{\pm}$. First note that by Proposition 3.2 and Proposition 3.3 the truth assignment $\varphi_{\overline{H}}$ is correctly defined. Since H is a nonempty concept intent of $\mathbb{K}_{+}$, Proposition 3.2 together with the fact that $I_{\neq}$ is the relation of contranominal scale implies $H^{+} = \{g_{x_i} \mid x_i \in \overline{H}\} \cup \{g_{\neg x_i} \mid \neg x_i \in \overline{H}\}$. Now $H^{++} \cap \{C_1, C_2, \ldots, C_k\} = \emptyset$, hence for any C_i $(1 \leq i \leq k)$ there is some $g_l \in H^{+}$ such that $g_l \notin C_i^{+}$. According to the definition of $\mathcal{I}_{\mathcal{C}}$ the latter means that literal l belongs to clause C_i. Thus $f(\varphi_{\overline{H}}) = true$.

($\Leftarrow$) Let φ be a truth assignment and $f(\varphi) = true$. Define $H = \overline{H_{\varphi}}$. Note that $H^{+} = \{g_{x_i} \mid x_i \in H_{\varphi}\} \cup \{g_{\neg x_i} \mid \neg x_i \in H_{\varphi}\}$, because $\mathcal{I}_{\neq}$ is the relation of contranominal scale and $H \cap g_{C_j}^{+} = \emptyset, 1 \leq i \leq k$. Suppose that $C_i \in H^{++}$ for some $1 \leq i \leq k$. This is equivalent to $H^{+} \subseteq C_i^{+}$. Hence, by definition of $\mathcal{I}_{\mathcal{C}}$, there is no literal $l \in H_{\varphi}$ such that $l \in C_i$. Therefore, the clause C_i does not hold and this contradicts the fact that φ satisfies CNF f. Thus $H^{++} = H$ and H is a hypothesis. Since H does not contain any $\{C_i\}$, it must contain an additional minimal hypothesis. □

Corollary 3.5. *MHE cannot be solved in output polynomial time, unless $P = NP$.*

4 Dualizing monotone Boolean functions on lattices

Let f be a monotone Boolean function on a lattice $\mathcal{L}$. Without loss of generality we can assume that $\mathcal{L}$ is a concept lattice $\mathcal{L} = \mathfrak{B}(G, M, I)$ of the corresponding formal context $\mathbb{K} = (G, M, I)$. Then $A \subseteq B \Rightarrow f((A, A')) \leq f((B, B'))$. It is known that any monotone Boolean function on a lattice is uniquely given by its minimal 1-values, i.e. by the set $\mathcal{A} = \{(A, A') \mid (A, A') \in \mathfrak{B}, f((A, A')) = 1, f((B, B')) = 0 \ \forall B \subset A\}$. Define positive context $\mathbb{K}_{+} = \mathbb{K}$. Define negative context $\mathbb{K}_{-} = (G_{-}, M, I_{-})$ via its set of objects intents $G_{-} = \{g_A \mid (A', A) \in \mathcal{A}\}$ and ${g_A}^{-} = A$. In other words negative examples are precisely intents of minimal 1-values of f. Clearly set of minimal hypotheses of $\mathbb{K}_{\pm}$ is exactly the set of maximal 0-values of f.

Symmetrically, for a given positive and negative contexts $\mathbb{K}_{+}$ and $\mathbb{K}_{-}$ define context $\mathbb{K}_{+\cup -} = (G_{+} \cup G_{-}, M, I_{+} \cup I_{-})$. Let f be a monotone Boolean function on $\mathbb{K}_{+\cup -}$ that is given by its minimal 1-values $\mathcal{A} = \{(g^{-'}, g^{-}) \mid g \in G_{-}\}$ ($(\cdot)'$ – derivation operator of $\mathbb{K}_{+\cup -}$). It is not hard to see that the set of maximal 0-values of f is defined by the set of minimal hypotheses of $\mathbb{K}_{\pm}$.

From Corollary 3.5 it follows that the following problem cannot be solved in output polynomial time unless $P = NP$

Problem: Maximial false values enumeration (MFE)
INPUT: A formal context $\mathbb{K}$ and a set of minimal 1 values of monotone Boolean function f on the concept lattice of $\mathbb{K}$.
OUTPUT: Set of maximal 0 values of f.

Lemma 3.1 also implies that the dualization problem on a lattice given by a formal context can be solved in output polynomial time iff the corresponding duality (decision version of dualization) problem can be solved in polynomial time.

Note that in the case of Boolean lattice MFE problem is polynomially equivalent to Monotone Boolean Dualization and minimal 0 values in this case can be enumerated in

quasi-polynomial time $O(N^{o(\log N)})$, where N is $|input\ size| + |output\ size|$ (see [10]).

In database theory a closure of a set of attributes A is defined by means of iterated applications of functional dependencies with premises contained in A. Same type of closure, by means of implications instead of functional dependencies, is known in FCA. More precisely, applying $\mathrm{imp}(A) = A \cup \{B \mid D \to B, D \subseteq A\}$ iteratively to A by putting at each next step $A :: = \mathrm{imp}(A)$ until saturation, one obtains implicational closure of A, which is equal to A'' [11]. So, the set of all implications of a context defines the closure operator $(\cdot)''$, closed subsets of attributes, which together with the respective closed subsets of objects (extents) give the concept lattice. Hence, instead of defining a lattice by the ordered set of its irreducible elements, one can define it in terms of the set of all valid implications of the respective formal context, or, equivalently, by its implication base. This consideration poses another setting of the dualization problem, where the lattice – instead of the set of positive examples G_+ – is given by its implications or implication base, and one has to dualize the monotone function given by the set of examples G_-. When the lattice is Boolean, its implication base is empty [11], so one has to dualize the set of examples G_-, which can be considered as a monotone DNF, where disjunction goes over objects – elements of G_- – which themselves can be taken as conjunctions of the respective attributes. When the lattice is distributive, its minimum implication base has one-element premises [11] (hence, the number of implications in the base is not larger than $|M|$), so it can easily be computed from the context in polynomial time, and vice versa. Therefore, the dualization on lattices given by implication bases for distributive lattices is polynomially equivalent to the dualization on lattices given by contexts (ordered sets of irreducible elements), which we study in the next section. The study of dualization problems for lattices given by implication bases is motivated by simple linear-time reciprocal translations of implications to functional dependencies [18] and propositional Horn theories [4].

In [15] it has been proven that the following problem is NP-hard:

Problem: Incremental maximal model (IME)
INPUT: Horn theory Φ and a set of its maximal models S.
QUESTION: Is there another maximal model of Φ not contained in S?

In terms of FCA a Horn theory corresponds to a set of implications $\mathcal{J}$ and maximal models correspond to inclusion maximal closed sets of $\mathcal{J}$, or object intents, that are not M. In the dualization setting maximal closed sets are dual to the singleton set $\{M\}$. Hence for the

Problem: Minimal true values enumeration, on lattice given by implication base (MTEIB)
INPUT: A lattice $\mathcal{L}(\mathcal{J})$ given by an implication base $\mathcal{J}$ and a set of maximal 0 values of monotone Boolean function f on the lattice $\mathcal{L}(\mathcal{J})$.
OUTPUT: Set of minimal 1 values of f.

we have the following

Corollary 4.1. *A solution of MTEIB is impossible in output polynomial time unless $P = NP$.*

5 Dualization and minimum implication bases

In this section we give complexity upper bounds of some important special cases of monotone Boolean dualization on lattices in terms of the complexity of minimum implication base problem (i.e. minimum Horn theory).
Problem: Minimum implication base recognition (MIBR)
INPUT: Formal context $\mathbb{K} = (G, M, I)$, set of implications $\mathcal{J}$.
QUESTION: Is $\mathcal{J}$ implication base of $\mathbb{K}$?

The complexity of MIBR problem is a long standing open problem. The only known complexity result is that MIBR is at least hard as monotone Boolean duality [21, 4].

As we have shown monotone Boolean duality on a lattice given by a formal context is coNP-complete. It turns out that if we additionally have an implication base as input then the problem does not get harder than MIBR.
Problem: Duality over lattices given by formal context and implication base (DCI)
INPUT: formal context $\mathbb{K} = (G, M, I)$, antichains $\mathcal{A}, \mathcal{B} \subseteq \mathcal{L}(\mathbb{K})$ satisfying (*), implication base $\mathcal{J}$ of $\mathcal{L}(\mathbb{K})$.
QUESTION: Are $\mathcal{A}$ and $\mathcal{B}$ dual on $\mathcal{L}(\mathbb{K})$?

Note that $\mathcal{J}$ could be any implication base of $\mathbb{K}$ that is not necessary minimum. Now we describe polynomial (Karp-)reduction of DCI to MIBR. Let us define a context $\mathbb{K}_{\mathcal{B}} = (G_{\mathcal{B}}, M, I_{\mathcal{B}})$, where $G_{\mathcal{B}} = \{g_B \mid g \in G, B \in \mathcal{B}\}$ ($|G_{\mathcal{B}}| = |G| \times |\mathcal{B}|$), and relation $I_{\mathcal{B}}$ is defined via object intents $g'_B = g' \cap B$ for any $g_B \in G_{\mathcal{B}}$. Obviously, a set $X \subseteq M$ is closed in $\mathbb{K}_{\mathcal{B}}$ iff X is closed in $\mathbb{K}$ and there is $B \in \mathcal{B}$ that $X \subseteq B$. Define implication base $\mathcal{J}_{\mathcal{A}} = \mathcal{J} \cup \{A \to M \mid A \in \mathcal{A}\}$. Clearly, a set X is closed (satisfied) in $\mathcal{J}_{\mathcal{A}}$ iff $X = M$ or X is closed in $\mathbb{K}$ and $A \nsubseteq X$ for any $A \in \mathcal{A}$. Thus $\mathcal{A}$ and $\mathcal{B}$ are dual on $\mathcal{L}(\mathbb{K})$ iff $\mathcal{J}_{\mathcal{A}}$ is implication base of $\mathbb{K}_{\mathcal{B}}$. We have proven:

Lemma 5.1. *MIBR is DCI-hard (under polynomial Karp-reduction)*

In [5, 7] the problem of dualization over product of lattices was considered. For the case of semi-lattices of bounded width Elbassioni has shown that the duality problem can be solved in quasi-polynomial time. Nevertheless in case of product of general lattices the existence of quasi-polynomial algorithm is still an open problem. Here we prove that this problem is not harder than MIBR.
Problem: Duality over product of lattices (DPL)
INPUT: Product of lattices $\mathcal{L} = \mathcal{L}_1 \times \ldots \times \mathcal{L}_k$ given by $\mathcal{L}_1, \ldots, \mathcal{L}_k$, antichains $\mathcal{A}, \mathcal{B} \subseteq \mathcal{L}$ satisfying (*),
QUESTION: Are $\mathcal{A}$ and $\mathcal{B}$ dual over $\mathcal{L}$?

Proposition 5.2. *MIBR is DPL-hard (under polynomial Karp-reduction)*

Proof. First note that given a lattice $\mathcal{L}_i$ (e.g. as a whole relation matrix) we can find all join-irreducible and meet-irreducible elements of $\mathcal{L}_i$ in $poly(|\mathcal{L}_i|)$ time. Thus it is possible to get context $\mathbb{K}_{\mathcal{L}_i} = (G_i, M_i, I_i)$ that defines lattice $\mathcal{L}_i$ in polynomial time. In order to construct a formal context $\mathbb{K}_{\mathcal{L}} = (G, M, I)$ of the product of lattices $\mathcal{L}$, we define $G = G_1 \sqcup \ldots \sqcup G_k$, $M = M_1 \sqcup \ldots \sqcup M_k$, and relation I. Without loss of generality let $g \in G_i$ and $m \in M_j$ then gIm iff $i \neq j$ or gI_im. It is straightforward to check that $\mathcal{L}(\mathbb{K})$ is isomorphic to $\mathcal{L}$.

In [20] (Lemmas A.2 and A.3) it was proven that (in FCA terms) *Given a formal context* $\mathbb{K} = (G, M, I)$ *one can compute its cardinality-minimum implication base* $\mathcal{J}$ *in* $O(|M|^2|\mathcal{L}(\mathbb{K})|^2)$ *time. Moreover, such a* $\mathcal{J}$ *contains at most* $|M|^2|\mathcal{L}(\mathbb{K})|$ *implications.* Thus for a given lattice $\mathcal{L}_i$ we can find implication base $\mathcal{J}_i$ of size $O(poly(|\mathcal{L}_i|)$ in time $O(poly(|\mathcal{L}_i|))$. Clearly, $\mathcal{J}_1 \cup \ldots \cup \mathcal{J}_k$ is an implication base of $\mathbb{K}_{\mathcal{L}}$. The proposition statement follows from Lemma 5.1. □

Another interesting special case of lattices for which we can establish similar complexity bound is the case of distributive lattices. It is known that for a given context $\mathbb{K}$ of a distributive lattice, the minimum implication base of $\mathbb{K}$ has size polynomial in $|\mathbb{K}|$ and can be found in polynomial time ([11]). Thus MIBR is in P for a distributive lattice. The following Corollary is directly implied from this fact and Lemma 5.1:

Corollary 5.3. *Dualization on distributive lattice problem: Given formal context* $\mathbb{K}$ *of a distributive lattice and antichains* $\mathcal{A}, \mathcal{B} \subseteq \mathcal{L}(\mathbb{K})$ *satisfying (*), decide whether* $\mathcal{A}$ *and* $\mathcal{B}$ *are dual or not? Is not harder than MIBR (under polynomial Karp-reduction).*

6 Dualization over distributive lattices

We assume that a distributive lattice is represented as a lattice $\mathcal{L}(\mathcal{P})$ of downsets (order ideals) of a poset $\mathcal{P}$, and poset $\mathcal{P}$ is given by a matrix $n \times n$. It is well known that any distributive lattice has such a representation [1, 14, 11]. Note that one can use formal context representation of the distributive lattice as well, since the size of the corresponding formal context $(P, P, \leq)$ is polynomial in n, and our dualization algorithm is subexponential.

We treat the elements of $\mathcal{L} = \mathcal{L}(\mathcal{P})$ as subsets of $\mathcal{P}$ (since they are downsets of $\mathcal{P}$), so for two downsets $A, B \in \mathcal{L}(\mathcal{P})$ $A \leq B$ means that $A \subseteq B$. For an element $p \in \mathcal{P}$, the smallest (by set inclusion) downset that contains p is denoted by $\downarrow p$, and the smallest upperset (order filter) that contains p is denoted by $\uparrow p$. More generally, for any subset $X \subseteq \mathcal{P}$, by $\downarrow X$ we denote the smallest downset that contains X, i.e. $\downarrow X = \cup_{p \in X} \downarrow p$.

Let $\mathcal{A}$ and $\mathcal{B}$ be antichains of a distributive lattice $\mathcal{L}(\mathcal{P})$. Further on we will call a triple of the form $((\mathcal{A}, \mathcal{B}), \mathcal{P})$ dualization problem input. Note that in the degenerate cases where $\mathcal{A} = \emptyset$ or $\mathcal{B} = \emptyset$ the duality can easily be tested in polynomial time. If $\mathcal{A}$ is empty, then $\mathcal{B}$ is dual to $\mathcal{A}$ iff $\mathcal{B} = \{\mathcal{P}\}$. If $\mathcal{B}$ is empty, then $\mathcal{A}$ is dual to $\mathcal{B}$ iff $\mathcal{A} = \{\emptyset\}$. Let us call the algorithm that tests duality in these two degenerate cases *EasyTest((A,B),P).*

We will also use the notion of frequency of an element $p \in \mathcal{P}$. Let $\mathcal{C}$ be some set of subsets of $\mathcal{P}$ (i.e. $\mathcal{C} \subseteq 2^{\mathcal{P}}$), then the frequency of p in $\mathcal{C}$ is the fraction of elements of $\mathcal{C}$ that contain p:

Definition 6.1. $freq_{\mathcal{C}}(p) = |\{C \in \mathcal{C} \mid p \in C\}|/|\mathcal{C}|$.

Let us denote $\overline{\mathcal{C}} = \{\mathcal{P} \setminus C \mid C \in \mathcal{C}\}$, thus by definition $freq_{\overline{\mathcal{C}}}(p) = |\{C \in \mathcal{C} \mid p \notin C\}|/|\mathcal{C}|$.

For convenience we define the quantities $N = |\mathcal{A}| + |\mathcal{B}|$, and $m = \max_{p \in \mathcal{P}} (|\downarrow p| + |\uparrow p|)$ (note that $m \geq 2$).

6.1 Algorithm

Here we describe a subexponential algorithm for testing duality on a distributive lattice. The structure of the algorithm is close to that in [10]. The algorithm decomposes the initial problem instance into smaller instances and solves them recursively. In order to keep the total number of recursive calls subexponential at each decomposition step, the algorithm tries to select an element of $\mathcal{P}$ such that either it is *frequent* or it has a *large* fraction of successors of predecessors.

Algorithm 2 TestDuality$((\mathcal{A}, \mathcal{B}), \mathcal{P})$

Require: $\mathcal{A}, \mathcal{B} \subseteq \mathcal{L}(\mathcal{P})$
1: **if** $\mathcal{A} = \emptyset$ or $\mathcal{B} = \emptyset$ **then**
2: **return** EasyTest$((\mathcal{A}, \mathcal{B}), \mathcal{P})$
3: **end if**
4: $n \Leftarrow |\mathcal{P}|$
5: $m \Leftarrow \max_{p \in \mathcal{P}} (| \downarrow p | + | \uparrow p |)$
6: $N = |\mathcal{A}| + |\mathcal{B}|$
7: **if** $m > n^{1/3}$ **then**
8: $p \Leftarrow \arg\max_{p \in \mathcal{P}} (| \downarrow p | + | \uparrow p |)$
9: **else**
10: **if** $\max_{p \in \mathcal{P}} freq_{\mathcal{A}}(p) < \frac{1}{m \log_{4/3} N}$ **and** $\max_{p \in \mathcal{P}} freq_{\overline{\mathcal{B}}}(p) < \frac{1}{m^2 \log_{4/3} N}$ **then**
11: **return false**
12: **end if**
13: $p \Leftarrow \arg\max_{p \in \mathcal{P}} (\max(freq_{\mathcal{A}}(p), freq_{\overline{\mathcal{B}}}(p)))$
14: **end if**
15: **return** TestDuality$((\mathcal{A}_1^p, \mathcal{B}_1^p), \mathcal{P} \setminus \downarrow p) \wedge$ TestDuality$((\mathcal{A}_2^p, \mathcal{B}_2^p), \mathcal{P} \setminus \uparrow p)$

To describe decomposition performed by our algorithm we define the following four sets:

$$\mathcal{A}_1^p = \{A \setminus \downarrow p \mid A \in \mathcal{A}\},\ \mathcal{B}_1^p = \{B \setminus \downarrow p \mid p \in B,\ B \in \mathcal{B}\},$$

$$\mathcal{A}_2^p = \{A \mid p \notin A,\ A \in \mathcal{A}\},\ \mathcal{B}_2^p = \{B \setminus \uparrow p \mid B \in \mathcal{B}\}.$$

Note that $\mathcal{B}_1^p = \{B \setminus \downarrow p \mid \downarrow p \subseteq B,\ B \in \mathcal{B}\}$, and $\mathcal{A}_2^p = \{A \mid \uparrow p \cap A = \emptyset,\ A \in \mathcal{A}\}$.
The following lemma proves the correctness of *Algorithm 2*.

Lemma 6.1. *For any $p \in \mathcal{P}$, $\mathcal{A}$ and $\mathcal{B}$ are dual iff the following two conditions hold:*
$\mathcal{A}_1^p$ and $\mathcal{B}_1^p$ are dual on $\mathcal{L}(\mathcal{P} \setminus \downarrow p)$,
$\mathcal{A}_2^p$ and $\mathcal{B}_2^p$ are dual on $\mathcal{L}(\mathcal{P} \setminus \uparrow p)$

Proof. ($\Leftarrow$) Let us fix arbitrary $X \in \mathcal{L}$. Consider two possible cases: $p \in X$ and $p \notin X$. If $p \in X$ then since $\mathcal{A}_1^p$ and $\mathcal{B}_1^p$ are dual, either $A_1 \subseteq X \setminus \downarrow p$ for some $A_1 \in \mathcal{A}_1^p$, or $X \setminus \downarrow p \subseteq B_1$ for some $B_1 \in \mathcal{B}_1^p$. Clearly, $X \setminus \downarrow p \subseteq B_1$ implies $X \subseteq B_1 \cup \downarrow p \in \mathcal{B}$. On the other hand $A_1 \in \mathcal{A}_1^p$ implies that there is $A \in \mathcal{A}$ such that $A_1 = A \setminus \downarrow p$, and hence $A \subseteq X$ (since $\downarrow p \subseteq X$).

If $p \notin X$ then since $\mathcal{A}_2^p$ and $\mathcal{B}_2^p$ are dual either $A_2 \subseteq X \setminus \uparrow p$ for some $A_2 \in \mathcal{A}_2^p$, or $X \setminus \uparrow p \subseteq B_2$ for some $B_2 \in \mathcal{B}_2^p$. By definition $B_2 \in \mathcal{B}_2^p$ implies that there is $B \in \mathcal{B}$ such that $B_2 = B \setminus \uparrow p$. Note that $A_2 \in \mathcal{A}$, and $X = X \setminus \uparrow p \subseteq B_2 \subseteq B$.

($\Rightarrow$) Let us prove that $\mathcal{A}_1^p$ and $\mathcal{B}_1^p$ are dual. Consider arbitrary $X \in \mathcal{L}(\mathcal{P} \setminus \downarrow p)$. Because $\mathcal{A}$ and $\mathcal{B}$ are dual on $\mathcal{L}(\mathcal{P})$ either $A \subseteq X \cup \downarrow p$ for some $A \in \mathcal{A}$, or $X \cup \downarrow p \subseteq B$ for some $B \in \mathcal{B}$. If $A \subseteq X \cup \downarrow p$ then $A \setminus \downarrow p \subseteq X$ (since $\downarrow p \cap X = \emptyset$). If $X \cup \downarrow p \subseteq B$ then $X \subseteq B \setminus \downarrow p$, and by definition $B \setminus \downarrow p \in \mathcal{B}_1^p$. It is easy to check that $(\mathcal{A}_1^p, \mathcal{B}_1^p)$ has property $(*)$

Now we prove that $\mathcal{A}_2^p$ and $\mathcal{B}_2^p$ are dual. Consider arbitrary $X \in \mathcal{L}(\mathcal{P} \setminus \uparrow p)$. Note that $X \in \mathcal{L}(\mathcal{P})$. Because $\mathcal{A}$ and $\mathcal{B}$ are dual on $\mathcal{L}(\mathcal{P})$ either $A \subseteq X$ for some $A \in \mathcal{A}$, or $X \subseteq B$ for some $B \in \mathcal{B}$. If $A \subseteq X$ then $p \notin A$, and $A \in \mathcal{A}_2^p$. If $X \subseteq B$ then $X \subseteq B \setminus \uparrow p$ (since $\uparrow p \cap X = \emptyset$). It is easy to check that $(\mathcal{A}_2^p, \mathcal{B}_2^p)$ has property $(*)$.

□

The following lemma helps one to establish a lower bound on the frequency of the most frequent element of $\mathcal{P}$.

Lemma 6.2. *If $\mathcal{A}$ and $\mathcal{B}$ are dual then*

$$\sum_{A \in \mathcal{A}} (3/4)^{|A|/m^2} + \sum_{B \in \mathcal{B}} e^{-(n-|B|)/m} \geq 1$$

Proof. To prove this bound we use the 'method of expectations' similar to that in [10], but with a more tricky probability distribution. Suppose we fixed some probability distribution of $X \in \mathcal{L}$. Let us denote the expected number of $A \in \mathcal{A}, A \subseteq X$ by $E_{\mathcal{A}}$, and the expected number of $B \in \mathcal{B}, X \subseteq B$ by $E_{\mathcal{B}}$. Antichains $\mathcal{A}$ and $\mathcal{B}$ are dual iff for any $X \in \mathcal{L}$ either $A \subseteq X$, for some $A \in \mathcal{A}$, or $X \subseteq B$, for some $B \in \mathcal{B}$. Thus if $\mathcal{A}$ and $\mathcal{B}$ are dual, then $E_{\mathcal{A}} + E_{\mathcal{B}} \geq 1$. By linearity of expectations $E_{\mathcal{A}} = \sum_{A \in \mathcal{A}} E_A$, where E_A is probability that $A \subseteq X$. Similarly, $E_{\mathcal{B}} = \sum_{B \in \mathcal{B}} E_B$, where E_B is the probability that $X \subseteq B$. Unlike to the case of Boolean lattice, no analytical expression for E_A and E_B is known (even the existence of a polynomial approximation algorithm is an open question [3]), but we can find upper bounds for $E_A,\ A \in \mathcal{A}$ and $E_B,\ B \in \mathcal{B}$.

In order to generate random (but not uniform) element $X \in \mathcal{L}$ we select each $p \in \mathcal{P}$ with probability $1/m$. Suppose elements $p_1, p_2, \ldots, p_r$ have been selected, then the resulting downset $X \in \mathcal{L}$ is defined as $X = \downarrow p_1 \cup \downarrow p_2 \cup \ldots \cup \downarrow p_r$.

For a given downset $A \in \mathcal{A}$ let us bound the probability that $A \subseteq X$. To each $p \in \mathcal{P}$ we assign an event I_p such that $p \in X$. Note that $Pr(\overline{I_p}) \geq (1 - 1/m)^m \geq 1/4$ (since $m \geq 2$). Consider any maximum-cardinality set $\{a_1, a_2, \ldots, a_k\} \subseteq A$ such that events $I_{a_1}, I_{a_2}, \ldots, I_{a_k}$ are mutually independent. For any $a \in A$ event I_a happens only if some $q \geq a$ was selected, hence I_a is independent of all I_q for $q \notin \big\downarrow(\uparrow a)$. Since $|\big\downarrow(\uparrow a)| \leq m^2$ it is easy to see that $k \geq |A|/m^2$. Since event $A \subseteq X$ happens if $I_{a_1} \wedge I_{a_1} \wedge \ldots \wedge I_{a_k}$ we have $Pr(A \subseteq X) \leq \prod_{1 \leq i \leq k} (1 - Pr(\overline{I_{a_i}})) \leq (1 - 1/4)^{|A|/m^2}$.

To bound E_B, note that for any $B \in \mathcal{B}$, the probability $Pr(X \subseteq B) = Pr(X \cap (\mathcal{P} \setminus B) = \emptyset)$. This probability is exactly $(1 - 1/m)^{|\mathcal{P} \setminus B|} = (1 - 1/m)^{n - |B|} \leq e^{-(n-|B|)/m}$ □

Corollary 6.3. *If $\mathcal{A}$ and $\mathcal{B}$ are dual, then at least one of the following statements is true:*

- $\exists p \in \mathcal{P} : freq_{\mathcal{A}}(p) \geq \frac{1}{m \log_{4/3} N}$

- $\exists p \in \mathcal{P} : freq_{\overline{\mathcal{B}}}(p) \geq \frac{1}{m^2 \log_{4/3} N}$

Proof. Let $k_A = \min_{A \in \mathcal{A}} |A|/m^2$, $k_B = \min_{B \in \mathcal{B}} (n - |B|)/m$, and $k = \min(k_A, k_B)$. By Lemma 6.2 $\sum_{A \in \mathcal{A}} (3/4)^{|A|/m^2} + \sum_{B \in \mathcal{B}} (3/4)^{(n-|B|)/m} \geq 1$. Hence $(3/4)^k N \geq 1$ which yields $k \leq \log_{4/3} N$. Since $(\mathcal{A}, \mathcal{B})$ has property $(*)$, for any $A \in \mathcal{A}$, $B \in \mathcal{B}$ the intersection $A \cap \overline{B}$ is nonempty. If $|A| = km^2$, then there is some $a \in A$ such that $freq_{\overline{\mathcal{B}}}(a) \geq 1/(km^2) \geq 1/(m^2 \log_{4/3} N)$. Similarly, if $|\overline{B}| = km$, then there is some $b \notin B$ such that $freq_{\mathcal{A}}(b) \geq 1/(km) \geq 1/(m \log_{4/3} N)$. □

Theorem 6.4 (Time complexity of the dualization algorithm)**.** Algorithm 2 *decides duality in time* $2^{O(n^{0.67} \log^3(|\mathcal{A}|+|\mathcal{B}|))}$.

Proof. First note that all lines of *Algorithm 2* can be computed in polynomial time (disregarding recursive calls). In order to bound the number of recursive calls during an execution of *Algorithm 2*, we consider the following *problem volume* quantity: $vol(\mathcal{A}, \mathcal{B}, \mathcal{P}) = |\mathcal{A}| \cdot |\mathcal{B}| \cdot n$. Dualization problem $(\mathcal{A}, \mathcal{B}, \mathcal{P})$ branches into two subproblems $(\mathcal{A}_1^p, \mathcal{B}_1^p, \mathcal{P} \setminus \downarrow p)$ and $(\mathcal{A}_2^p, \mathcal{B}_2^p, \mathcal{P} \setminus \uparrow p)$. Let us denote the volumes of these problems by vol, vol_1, and vol_2, respectively. In case of `line` 13 by Corollary 6.3 either $vol_2 \leq (1 - \frac{1}{m \log N}) vol$ or $vol_1 \leq (1 - \frac{1}{m^2 \log N}) vol$. Moreover, in case of `line` 8 of the *Algorithm 2*, $m = |\downarrow p| + |\uparrow p| > n^{1/3}$, which implies either $vol_1 \leq (n - \frac{m}{2})/n \cdot vol \leq (1 - \frac{1}{2n^{2/3}}) vol$, or $vol_2 \leq (1 - \frac{1}{2n^{2/3}}) vol$. Thus, we have the following bound on the number of recursive calls: $A(vol) \leq A((1 - \frac{1}{2n^{2/3} log N}) vol) + A(vol - 1) + 1$. In [10] it has been proven that solution $A(v)$ of the recurrence $A(v) \leq 1 + A((1 - \varepsilon)v) + A(v - 1)$, $A(1) = 1$ can be bounded by $A(v) \leq (3 + 2v\varepsilon)^{\log v/\varepsilon}$. Substituting $\varepsilon = \frac{1}{2n^{2/3} log N}$ yields $A(v) \leq (3 + 2N^2 n^{1/3})^{O((\log N + \log n) n^{2/3} \log N)} \leq 2^{O((\log N + \log n)^2 n^{2/3} \log N)} \leq 2^{O(n^{0.67} \log^3 N)}$. □

7 Conclusion

In this paper we have studied the dualization problem on a lattice given by the ordered sets of its irreducible elements (i.e., as a concept lattice). For this representation, the dualization problem has complexity different from that in case of explicit lattice representation as an ordered set of all its elements. We have shown that the dualization problem for a lattice given by the ordered set of its irreducible elements (concept lattice) is equivalent to the enumeration of minimal hypotheses, which is not possible in output polynomial time unless P=NP. For the case of distributive lattices dualization was shown to be possible in subexponential time. We have proved that the long standing open complexity problem of constructing minimum implication base (irredundant Horn CNF) is at least as hard as dualization over distributive lattice or dualization over the product of explicitly given lattices (open problem stated by Elbassioni [7]).

It is still open whether dualization over distributive lattice can be solved in output quasi-polynomial time, or this problem cannot be solved in output polynomial time unless P = NP. The complexity of dualization for other important classes of lattices, such as modular, also remains an open question for the case where the lattice is given by the ordered set of its irreducible elements.

Acknowledgments

We thank Kazuhisa Makino and Lhouari Nourine for helpful discussions. The second author was supported by the Basic Research Program of the National Research University Higher School of Economics (Moscow, Russia) and Russian Foundation for Basic Research.

References

[1] B.A. Davey, H.A. Priestley, Introduction to Lattices and Order, University of Oxford, 2002.

[2] J.L. Guigues and V. Duquenne, Familles minimales d'implications informatives resultant d'un tableau de données binaires, *Mathématiques, Informatique et Sciences Humaines*; 95:5-18, (1986).

[3] M. Dyer, L. A. Goldberg, C. Greenhill, M. Jerrum, *The Relative Complexity of Approximate Counting Problems*, Algorithmica (2004), vol 38, pp. 471-500.

[4] T. Eiter, K. Makino, G. Gottlob, Computational Aspects of Monotone Dualization: A Brief Survey, Discrete Applied Mathematics 156 (2008) 2035-2049.

[5] K.M. Elbassioni: An Algorithm for Dualization in Products of Lattices and Its Applications. Proc. 10th Annual European Symposium (ESA 2002), Eds. R. Möhring, R.Raman, Lecture Notes in Computer Science, Springer, vol. 2461, pp 424-435.

[6] K.M. Elbassioni, *On Dualization in Products of Forests*, STACS 2002, pp 142-153.

[7] K.M. Elbassioni, *Algorithms for Dualization over Products of Partially Ordered Sets*, SIAM J. Discrete Math. 23(1) (2009), pp. 487-510

[8] V. K. Finn, *On Machine-Oriented Formalization of Plausible Reasoning in the Style of F. Backon–J. S. Mill*, Semiotika Informatika (1983), vol. 20, pp. 35-101 [in Russian].

[9] V. K. Finn, *Plausible Reasoning in Systems of JSM Type*, Itogi Nauki i Tekhniki, Seriya Informatika (1991), vol. 15, pp. 54-101, [in Russian].

[10] M. L. Fredman and L. Khachiyan, *On the Complexity of Dualization of Monotone Disjunctive Normal Forms*, Journal of Algorithms (1996), vol. 21, pp. 618-628.

[11] B. Ganter and R. Wille, *Formal Concept Analysis: Mathematical Foundations*; Springer, Berlin (1999).

[12] M. Garey and D. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*; Freeman, San Francisco (1979).

[13] B. Ganter and S.O. Kuznetsov, *Hypotheses and Version Spaces*, Proc. 10th Int. Conf. on Conceptual Structures, ICCS'03, A. de Moor, W. Lex, and B.Ganter, Eds., Lecture Notes in Artificial Intelligence, vol. 2746 (2003), pp. 83-95.

[14] G. Grätzer, *Lattice Theory: Foundation*, Birkhäuser (2011).

[15] D. J. Kavvadias, M. Sideri, E. C. Stavropoulos, *Generating All Maximal Models of a Boolean Expression*, Inf. Process. Lett. (2000), 74(3-4), pp. 157-162.

[16] S.O. Kuznetsov, *Mathematical Aspects of Concept Analysis*, Journal of Mathematical Science (1996), Vol. 80, Issue 2, pp. 1654-1698.

[17] S.O. Kuznetsov, *Complexity of Learning in Concept Lattices from Positive and Negative Examples*, Discrete Applied Mathematics (2004), no. 142, pp. 111-125.

[18] S.O.Kuznetsov, S.A.Obiedkov, *Some Decision and Counting Problems of the Duquenne-Guigues Basis of Implications*, Discrete Applied Mathematics (2008), vol. 156, no. 11, pp. 1994-2003.

[19] L. Nourine, J.-M. Petit, *Extending Set-based Dualization: Application to Pattern Mining*, In Luc de Raedt, Ed., Proc. European Conference on Artificial Intelligence (ECAI'2012), pp. 630-635 (2012).

[20] R. Dechter, J. Pearl, *Structure Identification in Relational Data*, Artificial Intelligence, 5 (1992), pp. 237-270.

[21] R. Khardon, *Translating between Horn Representations and Their Characteristic Models*, J. Artif. Intell. Res. (JAIR) 3, (1995), pp. 349-372.